



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/582,831

04/12/2007

Hans Wyssen

27592-01057-US3

4997

30678

7590

05/11/2009

CONNOLLY BOVE LODGE & HUTZ LLP

1875 EYE STREET, N.W.

SUITE 1100

WASHINGTON, DC 20006

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

05/11/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/582,831	<b>Applicant(s)</b> WYSSEN, HANS	
	<b>Examiner</b> KAVEH ABRISHAMKAR	<b>Art Unit</b> 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 08 January 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the amendment filed on January 8, 2009. Claims 1-38 were originally pending consideration. Per the received amendment, no claims were cancelled or added.
2. Claims 1-38 are currently being considered.

### ***Response to Arguments***

Applicant's arguments filed on January 8, 2009 have been fully considered but they are not persuasive for the following reasons:

The Applicant argues that the Cited Prior Art (CPA), Pasieka (U.S. Patent 6,587,945), does not teach that the original document has an electronic, verifiable provenance. This argument is not found persuasive. A "provenance" is defined as the origin or the source of something. Therefore, an electronic, verifiable provenance, would be an electronic or digital verifiable source. The CPA discloses that an image is created and stored at the server, wherein the imager ID or author ID are used along with an image sequence number, and that the author private key, is used to create an image signature (column 4, lines 17-55). The author ID is the source or origin of the image, is analogous to the provenance, and the private key is also evidence of the source or origin of the image. This image signature which uses the author's private key and/or the author ID, is analogous to a provenance as it is evidence of the source or

Art Unit: 2431

destination of the image. Furthermore, the CPA discloses that "the purpose of the encryption is to provide proof that the author is the originator of the image, and that the image has not been altered by others since it was signed" (column 4, lines 49-57).

Therefore, the provenance (origin) of the image would be verified, and since the invention takes place on a computer system, wherein the image can be a scanner, camera (column 4, lines 15-25), it is also electronic.

Therefore, the rejection for the claims is maintained as given below.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-15, 17-34, 36 and 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Pasieka (U.S. Patent 6,587,945).

Regarding claim 1, Pasieka discloses:

A computer system accessible remotely by a user to authenticate a document, comprising:

a memory configured to store electronic image data corresponding to an original document having an electronic displayable verifiable provenance (column 4, lines 13-18: *server stores the image*), and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document (column 4, lines 49-55: *form an image signature*), and

an output configured to provide said image data and said verification information for display by the user to authenticate the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the image data has been obtained from an authenticated source, and the verification information includes data corresponding to the provenance of the authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein data is fed to and from the memory under the control of a repository (column 4, lines 13-15: *servers signs and stores the image, and then can submit the image to another secure server*).

Art Unit: 2431

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Pasioka discloses:

A computer system according to claim 3 wherein the verification information comprises data concerning the provenance that has been subjected to authentication by the repository, and the verification information being configured to signal to the user that the repository provides such authentication (column 4, lines 50-55, column 5, lines 4-9: *digital signature of the image to prove the origin*).

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Pasioka discloses:

A computer system according to claim 2 wherein data stored in the memory cannot be altered by users (column 4, lines 48-55: *image is encrypted then stored so it cannot be altered*).

Claim 6 is rejected as applied above in rejecting claim 3. Furthermore, Pasioka discloses:

A computer system according to claim 3 including apparatus to receive the image data from a remote location (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Pasioka discloses:

Art Unit: 2431

A computer system according to claim 1 including a scanner for scanning an original document to produce said image data (column 4, lines 15-24: *imager can include a scanner*).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 including a repository agent including apparatus operable to send image data corresponding to an original image to the repository (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Pasieka discloses:

A computer system according to claim 8 wherein the repository agent is operable to send the image data together with source authentication information to indicate to the repository that the image data has been sent from the agent (column 4, lines 30-35: *the transmission will identify the author and the imager device*).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the verification information comprises predetermined accreditation indicia to be viewed by a user concurrently with

Art Unit: 2431

the image data for authenticating individual parts of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Pasioka discloses:

A computer system according to claim 1 wherein the verification information comprises accreditation data to be viewed by a user in a separate field associated with the image data for authenticating the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Pasioka discloses:

A computer system according to claim 1 wherein the image data and the verification information are stored in a common electronic file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Pasioka discloses:

A computer system according to claim 12 wherein the file is a PDF file (column 4, lines 17-25: *wherein the image can be any file*).



Art Unit: 2431

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 including a server providing said memory and operable to host a website at which said image data and verification information is viewable by a user to authenticate the original document (column 5, lines 55-67: *wherein a server is used to view the images, and wherein it is inherent that the server can act like a web server*).

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein said output is connected to the Internet (column 4, lines 27-29: *image can be sent over a public network*).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses;

A computer system according to claim 1 wherein said image data and verification information in the memory is password protected so that the user can only gain access thereto by use of the password (column 5, lines 10-13: *wherein there are different password pairs*).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

Art Unit: 2431

A computer system according to claim 1 wherein the image data and the verification information corresponding to the original document when stored in the memory collectively has an individual addressable identity (column 4, lines 31-35: *image record stored with an image ID*).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A method of operating a computer system according to claim 1 to provide said image data and said verification information for display by the user to authenticate the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Regarding claim 19, Pasieka discloses:

A method of displaying a document for authentication, comprising:

creating electronic image data corresponding to an original document having an electronic displayable verifiable provenance (column 4, lines 15-24: *imager can include a scanner*),

providing electronic, displayable verification information corresponding to the provenance of at least part of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*), and

Art Unit: 2431

displaying the image data and the verification information, to permit a user to authenticate the document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Pasioka discloses:

A method according to claim 19 including receiving the image data from an authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*), storing the image data for display (column 4, lines 13-18: *server stores the image*), and creating the verification information for the received image (column 4, lines 49-55: *form an image signature*), wherein the verification information includes data corresponding to the provenance of the authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 21 is rejected as applied above in rejecting claim 19. Furthermore, Pasioka discloses:

A method according to claim 19 including authenticating the source of the image data (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 22 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

Art Unit: 2431

A method according to claim 18 including feeding the image data and the verification information to a memory under the control of a repository for display to users wishing to authenticate the original document (column 4, lines 13-15: *servers signs and stores the image, and then can submit the image to another secure server*).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Pasioka discloses:

A method according to claim 22 wherein only the repository can change the data in the memory (column 4, lines 48-55: *image is encrypted then stored so it cannot be altered*).

Claim 24 is rejected as applied above in rejecting claim 22. Furthermore, Pasioka discloses:

A method according to claim 22 wherein the verification information comprises data concerning the provenance that has been authenticated by the repository (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Pasioka discloses:

A method according to claim 24 wherein the repository communicates with the source of the image data to determine the provenance thereof and to develop said

Art Unit: 2431

verification information (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 26 is rejected as applied above in rejecting claim 22. Furthermore, Pasioka discloses:

A method according to claim 22 including feeding the image data to the repository from a remote location (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 27 is rejected as applied above in rejecting claim 22. Furthermore, Pasioka discloses:

A method according to claim 22 including sending send image data corresponding to an original image from a repository agent to the repository (column 4, lines 12-15: *image is originally sent to a server which signs and stores it*).

Claim 28 is rejected as applied above in rejecting claim 26. Furthermore, Pasioka discloses:

A method according to claim 26 including sending the image data together with source authentication information to indicate to the repository that the image data has been sent from the repository agent (column 4, lines 30-35: *the transmission will identify the author and the imager device*).

Art Unit: 2431

Claim 29 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including configuring the verification information to include predetermined accreditation indicia viewable concurrently with the image data for authenticating individual parts of the original document by a user that authenticates the document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 30 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including configuring the verification information to comprise accreditation data to be viewable by a user in a separate field associated with the image data for authenticating the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 31 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including storing the image data and the verification information are stored in a common electronic file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 32 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including storing the image data and the verification information are stored in a common electronic PDF file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 33 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including hosting a website at which said image data and verification information is viewable by a user to authenticate the original document (column 5, lines 55-67: *wherein a server is used to view the images, and wherein it is inherent that the server can act like a web server*).

Claim 34 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses:

A method according to claim 18 including authenticating the original document by viewing said electronic image data and the corresponding verification information (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 35 is rejected as applied above in rejecting claim 18. Furthermore, Pasioka discloses;

A method according to claim 18 wherein said image data and verification information is password protected so that a user can only gain access thereto by use of the password, and including supplying the password to a user to permit the user to

Art Unit: 2431

authenticate the original document (column 5, lines 10-13: *wherein there are different password pairs*).

Claim 36 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 wherein the image data and the verification information corresponding to the original document collectively have an individual addressable identity and including supplying the individual addressable identity to a user to permit the user to access the data and information for authenticating the original document (column 4, lines 31-35: *image record stored with an image ID*).

Claim 37 is rejected as applied above in rejecting claim 35. Furthermore, Pasieka discloses:

A method according to claim 35 including supplying a hyperlink to the user (column 5, lines 10-13: *wherein there are different password pairs, and it is well-known to supply information via hyperlinks*)

Regarding claim 38, Pasieka discloses:

A computer system comprising:  
a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to



Art Unit: 2431

authenticate the document (column 4, lines 10-40), wherein the electronic signal comprises:

an electronic image data corresponding to an original document having a verifiable provenance (column 4, lines 13-18: *server stores the image*), and

electronic, displayable verification information corresponding to the provenance of at least part of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

Art Unit: 2431

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/  
Primary Examiner, Art Unit 2431

/K. A./  
05/07/2009  
Primary Examiner, Art Unit 2431